arXiv:quant-ph/0601142v1 21 Jan 2006

Secret sharing of quantum information via entanglement swapping in cavity QED*

Ying-Qiao Zhang, Xing-Ri Jin, Shou Zhang†

Department of Physics, College of Science,

Yanbian University, Yanji, Jilin, 133002, China

We proposed a scheme on secret sharing of quantum information based on entanglement swapping in cavity QED. In our scheme, the effects of cavity decay and thermal field are all eliminated.

PACS numbers: 03.67.Dd; 03.65.Ud

Keywords: Secret sharing, Entanglement swapping, Cavity QED

I. INTRODUCTION

Using the theory of quantum mechanics in the field of information in the recent years has produced many interesting developments, such as quantum teleportation[1], quantum cryptography[2], quantum secret sharing (QSS)[3], and so on. Quantum secret sharing, firstly proposed by Hillery *et al*[3], is one of the basilic components of quantum communication and is used to fulfill the task of classical secret sharing. The basic idea of secret sharing, invented by both Shamir[4] and Blakely[5] independently in 1979, is to distribute a secret between n players in such a way that any group of k or more players can together reconstruct the secret but no group of less than k players can know anything about the secret even if they cooperate. Such a system is called a (k, n)-threshold scheme. The property of QSS, being used to share both classical information and quantum information, makes it differ from the classical secret sharing. QSS scheme can be used in joint sharing of quantum money[6], sharing difficult-to-construct ancilla states[7], and so on.

Therefore, many attentions[8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21] have been concentrated on the realization of QSS both in theory and experiment using many kinds of methods. Entanglement swapping is one of the methods being used in QSS protocols[16,

* Foundation item: Supported by the National Science Foundation of China under Grant (60261002).

† E-mail: szhang@ybu.edu.cn

22, 23]. Zhang *et al*[22] and Li *et al*[23] proposed multi-party quantum secret sharing protocols based on entanglement swapping using the Bell-state measurements and GHZ-basis measurements, respectively. But performing the Bell-state measurements and GHZ-basis measurements in QSS scheme is difficult, so we propose a scheme to realize the QSS in cavity QED via entanglement swapping. We know that a (k, n)-threshold scheme requires that no single player can have any information on the unknown state if they act alone. So our scheme isn't the conventional quantum (k, n)-threshold scheme, because each player has the amplitude information of the unknown state. In Section II, we discuss the secret sharing protocol in three-party system, and the generalization to multi-party system is given in Section III.

II. THREE-PARTY QUANTUM INFORMATION SECRET SHARING

We consider the three-party system consists of Alice, Bob, and Charlie. At first, Alice possesses six atoms, namely, atom 1, atom 2,..., atom 6. The state of atom 1 that Alice wants to send to Bob and Charlie is

$$|\Psi\rangle_1 = \alpha|e\rangle_1 + \beta|g\rangle_1, \tag{1}$$

where α and β are unknown coefficients, they satisfy $|\alpha|^2 + |\beta|^2$=1. $|e\rangle$ and $|g\rangle$ are atom excited and ground states, respectively. The states of atoms 2, 3, 4, and 5, 6 are in three-atom maximally entangled state and two-atom maximally entangled state, respectively, as

$$|\Psi\rangle_{234} = \frac{1}{\sqrt{2}}(|eee\rangle_{234} + |ggg\rangle_{234}), \tag{2}$$

$$|\Psi\rangle_{56} = \frac{1}{\sqrt{2}}(|ee\rangle_{56} + |gg\rangle_{56}). \tag{3}$$

We consider the atoms 1, 2, 3, 4, 5, and 6 are all identical two-level atoms. The joint state of the six atoms can be expressed as

$$|\Psi\rangle = |\Psi\rangle_1 \otimes |\Psi\rangle_{234} \otimes |\Psi\rangle_{56}. \tag{4}$$

Firstly, Alice introduces two identical single-mode cavities and simultaneously sends the atoms 1, 2 and atoms 3, 5 into the two single-mode cavities, respectively. So there are two interaction systems of atoms and cavity in all. Considering the two atoms 1, 2 (3,

5) simultaneously interacting with the single-mode cavity field and driving by the classical field, respectively.

The interaction Hamiltonian between the atoms and the single-mode cavity is[24] ($\hbar = 1$)

$$H = \omega_0 \sum_{j=1}^{2} S_{z,j} + \omega_1 a^\dagger a + \sum_{j=1}^{2} [g(a^\dagger S_j^- + a S_j^\dagger) + \Omega(S_j^\dagger e^{-i\omega_2 t} + S_j^- e^{i\omega_2 t})], \tag{5}$$

where $S_j^- = |g\rangle_{jj}\langle e|$, $S_j^\dagger = |e\rangle_{jj}\langle g|$, $S_{z,j} = \frac{1}{2}(|e\rangle_{jj}\langle e| - |g\rangle_{jj}\langle g|)$, $|e\rangle_j$ and $|g\rangle_j$ are the excited and ground states of the jth atom, $a^\dagger$ and a are creation operator and annihilation operator of the cavity mode. g is the coupling constant between the atoms and cavity, ω_0, ω_1, ω_2 are atomic transition frequency ($e \leftrightarrow g$), cavity frequency, driving field frequency, respectively, and Ω is the Rabi frequency of the classical field. We consider the atomic transition frequency equals to driving field frequency ($\omega_0 = \omega_2$). In the case of large detuning $\delta \gg g/2$ and strong driving field $2\Omega \gg \delta$ (g limit), the effective Hamiltonian of the interaction system can be expressed as[25]

$$H_{\text{eff}} = \frac{\lambda}{2}[\sum_{j=1}^{2}(|e\rangle_{jj}\langle e| + |g\rangle_{jj}\langle g|) + \sum_{j,k=1,j\neq k}^{2} (S_j^\dagger S_k^\dagger + S_j^\dagger S_k^- + \texttt{H.c.})], \tag{6}$$

where $\lambda = g^2/2\delta$ with δ being the detuning between ω_0 and ω_1. So the effects of cavity decay and thermal field are all avoided. The evolution operator of the system in interaction picture can be expressed as

$$U(t) = e^{-iH_0 t} e^{-iH_{\text{eff}} t}, \tag{7}$$

where $H_0 = \sum_{j=1}^{2} \Omega(S_j^\dagger + S_j^-)$.

We consider the interaction time of atoms 1, 2 with the single-mode cavity and the interaction time of atoms 3, 5 with the single-mode cavity are the same. After the interaction, Alice sends atoms 4 and 6 to Bob and Charlie, respectively. When she is sure that Bob and Charlie have both receive an atom, she measures on atoms 1, 2, 3, 5 and informs Bob and Charlie of her measurement results via a public channel. If the measurement result is $|eeee\rangle_{1235}$, the state of atoms 4, 6 collapses into

$$|\Psi\rangle_{46} = \alpha|ee\rangle_{46} - \beta|gg\rangle_{46}, \tag{8}$$

by selecting the interaction time satisfy $\lambda t = \frac{\pi}{4}$ and making the Rabi frequency satisfy $\Omega t = \pi$. Here we must emphasize that the net effect of the evolution is to apply a σ_z to the unknown state and then to apply a CNOT to the unknown state and a standard $|g\rangle$, namely $\sigma_z(\alpha|e\rangle + \beta|g\rangle) = \alpha|e\rangle - \beta|g\rangle$, CNOT$\rightarrow (\alpha|e\rangle - \beta|g\rangle)|g\rangle = \alpha|ee\rangle - \beta|gg\rangle$.

Now Alice has successfully transferred the quantum information to Bob and Charlie by entanglement swapping, so the distribution of quantum information is completed.

We observe that neither Bob nor Charlie can recover the state $|\Psi\rangle_1$ in its exact form by performing any general operations themselves without communicating between themselves. Though they have the amplitude information, that is not sufficient since the phase information is not available. In this case they must agree to cooperate among themselves. Only by this way, one of them, not both, can recover the desired state for the no-cloning theorem.

We rewrite the state $|\Psi\rangle_{46}$ in Eq.(8), as

$$|\Psi\rangle_{46} = \frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|e\rangle_4 + |g\rangle_4)(\alpha|e\rangle_6 - \beta|g\rangle_6) + \frac{1}{\sqrt{2}}(|e\rangle_4 - |g\rangle_4)(\alpha|e\rangle_6 + \beta|g\rangle_6)]. \quad (9)$$

If Alice assigns Charlie to recover the quantum state in Eq.(1), then Bob needs to measure on atom 4 in the X-basis, where the X-eigenstates are defined by

$$|X^{\pm}\rangle = \frac{1}{\sqrt{2}}(|e\rangle \pm |g\rangle). \quad (10)$$

If Bob's measurement result is

$$|\Psi\rangle_4 = \frac{1}{\sqrt{2}}(|e\rangle_4 + |g\rangle_4), \quad (11)$$

according to Eq.(9), the state of atom 6 becomes

$$|\Psi\rangle_6 = \alpha|e\rangle_6 - \beta|g\rangle_6. \quad (12)$$

Then Bob communicates his outcome to Charlie in a public channel. At this stage, Charlie can recover the unknown state by performing the rotation operation σ_z on atom 6

$$\sigma_z|\Psi\rangle_6 = \alpha|e\rangle_6 + \beta|g\rangle_6. \quad (13)$$

So Charlie can recover the state $|\Psi\rangle_1$ with the help of Bob.

Now we discuss the security of our scheme. Suppose that there is an adversary, he will be either Bob or Charlie. The adversary (say, Bob) wants to eavesdrop Alice's information without being detected. If Alice assigns Bob to receive the state and Charlie agrees to cooperate with Bob, Bob can eavesdrop the state with a successful probability of 100 percent, and the cheating will not be detected. If Alice assigns Bob to receive the state and Charlie doesn't agree to cooperate with Bob, in this case Charlie doesn't tell Bob his measurement results. Bob can also eavesdrop the state, but the successful probability is only 50 percent,

he will still get nothing with a probability of 50 percent. However, if Alice assigns Charlie to receive the state, Bob will measure the state of his atom in the X basis and tell his measurement results to Charlie, Charlie can recover the state with the help of Bob. There is also the probability that Bob could lie about his measurement results. By doing so, Bob gains nothing and Charlie can't recover the correct state. Of course, Bob can also manage to get a hold of the atom that Alice sends to Charlie, and sends Charlie an atom that he has prepared. He wants to discover the state of Alice's atom 1 without the help of Charlie. In this way, only when Alice assigns him to recover the state, he can get the state of Alice's atom 1 without being detected. On the other hand, if Alice assigns Charlie to recover the state, then Bob has some trouble. Bob doesn't know Alice's measurement result and therefore the atom that he sends to Charlie is not in the correct quantum state. So the state recovered by Charlie will be different with the state Alice has sent. If Alice checks a subset of the state with Charlie publicly, the eavesdropping behavior can be revealed. The security of the present scheme is the same as that in contribution[23].

III. MULTI-PARTY QUANTUM INFORMATION SECRET SHARING

In this section, we generalize the three-party secret sharing scheme to multi-party system. At first, Alice possesses $3n$ identical two-level atoms, marked as: atom 1, atom 2,..., atom $3n$. The state of atom 1 that Alice wants to send to n users is still in Eq.(1). The states of atoms 2, 3,..., $(3n-2)$ are in the following $(n-1)$ three-atom maximally entangled states, respectively, as

$$|\Psi\rangle_{234} = \frac{1}{\sqrt{2}}(|eee\rangle_{234} + |ggg\rangle_{234}),$$

$$|\Psi\rangle_{567} = \frac{1}{\sqrt{2}}(|eee\rangle_{567} + |ggg\rangle_{567}),$$

$$|\Psi\rangle_{8,9,10} = \frac{1}{\sqrt{2}}(|eee\rangle_{8,9,10} + |ggg\rangle_{8,9,10}),$$

.....,

$$|\Psi\rangle_{3n-4,3n-3,3n-2} = \frac{1}{\sqrt{2}}(|eee\rangle_{3n-4,3n-3,3n-2} + |ggg\rangle_{3n-4,3n-3,3n-2}). \quad (14)$$

The state of atoms $(3n-1)$ and $(3n)$ is in the two-atom maximally entangled state

$$|\Psi\rangle_{3n-1,3n} = \frac{1}{\sqrt{2}}(|ee\rangle_{3n-1,3n} + |gg\rangle_{3n-1,3n}). \tag{15}$$

Firstly Alice simultaneously puts n pairs of atoms, namely, atoms (1, 2), atoms (3, 5), atoms (6, 8),..., atoms $(3n-3, 3n-1)$, into n identical single-mode cavities, respectively. So there are n interaction systems of atoms and cavity in all. Alice selects the same interaction time t for the n interaction systems. Secondly Alice sends the residual n atoms, namely, atom 4, atom 7, atom 10,..., atom $(3n-2)$, and atom $(3n)$, to each one of the n users, respectively. When she is sure that each one of the n users has received an atom, Alice measures on the n pairs of atoms that having been put into the cavities. The n users obtain a pure entangled state of the residual n atoms which contains all the information of the state in Eq.(1). So the distribution of the quantum information is completed. Then Alice publicly declares her measurement results and assigns one user (A) to receive the state. The rest $(n-1)$ users respectively perform an X-basis measurement as shown in Eq.(10) on their own atoms, and then inform the user (A) of their measurement results, respectively. So the user (A) can recover the state in Eq.(1) by performing appropriate rotation operation on his atom according to the information he has obtained from Alice and the rest $(n-1)$ users. The security of the multi-party secret sharing scheme is the same as that in Section II.

IV. SUMMARY

In the present scheme, the interaction system of atoms and cavity is in large detuning and strong driving field case, the effects of cavity decay and thermal field are all avoided, so the scheme is feasible with the present cavity QED techniques. In addition, when we treat the multi-party system, the n pairs of atoms must be sent simultaneously into n identical single-mode cavity fields, respectively. This will product errors between experiment operation and theory calculation. Because of the value of n is a finite number, the effects of the errors on the fidelity of the result state can be neglected.

In conclusion, we have presented a protocol of three-party quantum information secret sharing via entanglement swapping in cavity QED. Our scheme is easier to realize for without performing any Bell-state measurements and GHZ-basis measurements. This scheme can

also be generalized to the multi-party system.

---

[1] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70 (1993) 1895.

[2] A. K. Ekert, Phys. Rev. Lett. 67 (1991) 661.

[3] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A 59 (1999) 1829.

[4] A. Shamir, Communications of the ACM, 22 (1979) 612.

[5] G. Blakely, Proc. AFIPS, 48 (1979) 313.

[6] S. Wiesner, SIGACT News, 15 (1983) 78.

[7] D. Gottesman, I. Chuang, Nature, 402 (1999) 390.

[8] R. Cleve, D. Gottesman, and H. K. Lo, Phys. Rev. Lett. 83 (1999) 648.

[9] D. Gottesman, Phys. Rev. A 61 (1999) 042311.

[10] H. F. Chau, Phys. Rev. A 66 (2002) 060302.

[11] S. Bagherinezhad, V. Karimipour, Phys. Rev. A 67 (2003) 044302.

[12] V. Scarani, N. Gisin, Phys. Rev. Lett. 87 (2001) 117901.

[13] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. 92 (2004) 177903.

[14] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A 59 (1999) 162.

[15] S. Bandyopadhyay, Phys. Rev. A 62 (2000) 012308.

[16] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, Phys. Rev. A 65 (2002) 042320.

[17] G. P. Guo, G. C. Guo, Phys. Lett. A 310 (2003) 247.

[18] L. Xiao, G. L. Long, F. G. Deng, and J. W. Pan, Phys. Rev. A 69 (2004) 052307.

[19] F. G. Deng, G. L. Long, Y. Wang, and L. Xiao, Chin. Phys. Lett. 21 (2004) 2097.

[20] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A 63 (2001) 042301.

[21] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou, and Y. Wang, quant-ph/0501129.

[22] Z. J. Zhang, Z. X. Man, quant-ph/0406103.

[23] Y. M. Li, K. S. Zhang, and K. C. Peng, Phys. Lett. A 324 (2004) 420.

[24] M. Yang, Z. L. Cao, quant-ph/0411195.

[25] S. B. Zheng, Phys. Rev. A 68 (2003) 035801.